Frimley Health NHS
NHS Foundation Trust

Email Policy

Key Points

- The primary use of the Trust email is for work related purposes.
- Staff must NOT routinely send Personal Identifiable Data (PID) via email without encryption
- Staff must not send or forward offensive material or use the Trust email inappropriately. If they are found to be in breach of it they could be subjected to disciplinary action.
- Staff must not use their personal email for business use.
- The content of email is routinely monitored but the Trust reserves the right to access, read, print or delete emails at any time, i.e. the use of email is not private.
- Staff should be housekeeping their mailbox.

Version:	1.0
Role of Policy Lead(s):	Head of Information Governance
Role of Executive Lead:	SIRO
Date Approved by Executive Lead:	
Name of Responsible Committee:	IG Committee
Date Approved by Professional Approving Group:	15th September 2015
Date Approved by Policy Review Group:	(scheduled but not yet approved)
Date Ratified by Hospital Executive Board:	
Date Issued:	September 2015
Review Date:	September 2016
Target Audience:	All staff with an email account
Key Words & Phrases:	Email

Version Control Sheet

Version	Date	Policy Lead(s)	Status	Comment
1.0	10/09/2015	Nicola Gould	Draft	Revised policy following acquisition

Document Location

Document Type	Location
Electronic	Policy Hub (Trust-wide)
Paper	

Related Documents

Document Type	Document Name

1. INTRODUCTION

1.1. E-mail is an essential business tool, facilitating the sharing and dissemination of information between staff and beyond the Trust boundaries. Whilst it is critical to the effective operation of the Trust there are risks associated to its use, as has been demonstrated in highly publicised cases in the media.

1.2. All Trust staff are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply.

1.3. Frimley Health NHS Foundation Trust is committed to the provision of a service that is fair, accessible and meets the needs of all individuals.

2. SCOPE

2.1.1 This policy applies to all staff including Trust employees and non-Trust employees who work for the Trust. This includes, but is not limited to, staff on secondment to the Trust, contractors, students on placement and people working in a voluntary capacity.

2.1.2 This policy applies to the use of:

- NHS email accounts both nhs.uk and nhs.net for business and personal use on Trust and non-Trust premises including home and via portable media.
- The use of personal email accounts from Trust systems.

3. DEFINITIONS

3.1.1 Email: includes all features of MS Outlook – Inbox, Sent Items, Calendar and Tasks.

3.1.2 Legal Name: This is an individual's name as detailed on their birth certificate or marriage certificate.

4. PURPOSE OF THE POLICY

4.1.1 The purpose of the policy is to aid the effective and appropriate use of the Trust email systems and to reduce the risk of adverse events by;

- Setting out the standards that all staff must follow when using the Trust email system
- Ensuring the Trust email system is available for users by protecting it from unauthorised or accidental modification
- Preserve confidentiality and protect against unauthorised disclosure
- Making staff aware of what is acceptable and unacceptable use of the Trust's email system

5. THE POLICY

5.1.1 Every person using e-mail owned or operated by the Trust is responsible for complying with this policy and failure to comply with this policy may result in disciplinary action.

5.1.2 Email is a business communication tool and as such it must be used in a responsible, effective and lawful manner. Ownership of email boxes lies with the Trust and staff must be aware that the Trust reserves the right to read the content of any staff mail box.

5.1.3 The Trust provides access to email systems to employees and authorised non-Trust employees only for use in their:

- Work duties
- Work related educational purposes

- Work related research purposes

5.2 Patient Identifiable Data (PID).

5.2.1 Email is an insecure system. Therefore personal/sensitive personal information (e.g. that relating to patients or staff or other persons) or commercially sensitive information MUST NOT be sent externally by email unless it is encrypted to NHS standards using software approved by the Trust.

5.2.2 NHSmail (i.e. nhs.net) encrypts emails. Therefore it can be used to send personal/ sensitive personal/patient information to another NHSmail account (e.g. nhs.net to nhs.net).

5.2.3 However, personal/ sensitive personal/patient information sent from an NHSmail account to any other NHS email account e.g. fhft.nhs.uk is not secure and cannot be used to send personal/ sensitive personal/patient information. See Appendix 1.

5.2.4 Using NHSmail to send to another email address e.g. btinternet.com, doctors.net is not permitted as it is not secure.

5.2.5 Where patients have stated that they wish to communicate with Trust staff about their treatment via email, this is only permitted where the patient has consented and accepted the risks with this form of communication.

5.2.6 Guidance on obtaining consent to email patients about their care, can be found on the Trust's Information Governance intranet page.

5.2.7 Patient can be sent over the internal email service within the Trust, submit to the following guidelines:

- Patient information must be kept to a minimum
- There is a justified need to email patient information
- The patient's name is not placed in the subject heading of the email
- Staff must not forward on an email containing patient information to an insecure email address.

5.2.8 Personal/sensitive information (e.g. that relating to patients or staff or other persons) or commercially sensitive information MUST NOT be sent externally by email unless it is encrypted to NHS standards using software approved by the Trust.

5.3 Standard Rules of Email Use

5.3.1 Staff will be given a Trust email as per their legal name and the Trust's network access procedure.

5.3.2 Staff should ensure that they have selected the correct person before sending the email.

5.3.3 It is always good practice to use the spellchecker and re-read an email before sending it. Staff are advised to set up within Tools/Options/Spelling to "always check spelling before sending an email".

5.3.4 Staff must include in the signature of their email for at least all new emails, their full name, job title, contact telephone number and organisation.

5.3.5 To manage the size of a member of staff's outlook, staff should set up option within Outlook to automatically delete emails in the Deleted Items upon exiting Outlook.

5.3.6 Staff are responsible for managing their emails within their allocated size limit and this will entail creating folders to store emails that need to be kept and deleting emails that are no longer needed.

5.3.7 When out of the office, staff must activate the "Out of Office Assistant". The Out of Office message should include:

- The date when the member of staff will return to the office
- The name, contact details of the person to contact in their absence,
- The following FOI statement – "If your email relates to a Freedom of Information request, please forward your email to foi@fhft.nhs.uk."

5.3.8 Staff should remember that an email is a legal document and could be used as evidence in court and therefore should be factual.

5.3.9 Staff should ensure that the information held about them in Outlook Properties is accurate and up to date. Where a member of staff identifies that their information is inaccurate, then they need to log a call with the Informatics HelpDesk.

5.3.10 Users MUST report any third party email messages they receive about viruses to the Informatics HelpDesk immediately by telephone. The email must not be forwarded, or copied on to anyone, inside or outside the Trust network.

5.3.11 Staff experiencing problems receiving SPAM emails must contact the Informatics HelpDesk.

5.3.12 The Trust's email must not be used as the only method of communication if an urgent response is required.

5.3.13 Staff should not send large files via email e.g. attachments over 5MB as some email systems will reject emails that are over a set size. Where the Trust email system rejects an email due to its size, the user will be informed, however, this might not be the case with receiving email systems.

5.3.14 If staff wish to send an email attachment larger than 5MB they should contact the Informatics Help Desk to find alternative methods for sending an attachment of this size.

5.4 Monitoring of Emails

5.4.1 All information held or passed through the email system is monitored for viruses and is the property of the Trust.

5.4.2 The Trust reserve the right to monitor or intercept email communication, if required, in accordance with legislation such as:

- The Regulation of Investigatory Powers Act 2000,
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000,
- The Data Protection Act 1998,
- The Human Rights Act 1998

5.5 Global Email/Global Address Book

5.5.1 Only permitted members of staff can send global emails to all Trust staff.

5.5.2 Only permitted staff will be able to send an email to more than 100 staff at a time.

5.5.3 Global emails should not have any documents attached to it.

5.5.4 Where there is a justified need, non-Trust email addresses can be added to the Trust's Global email directory (address book). This will enable non Trust staff working in the Trust to receive critical Trust information. The criteria for requesting inclusion of a non-Trust email address are:

- Request must be submitted and sponsored by a Trust Manager
- Individuals must be from an organisation working in partnership with the Trust e.g. Social Services, etc.

- Addresses must be from valid professional/organisational domains (e.g. 'nhs.net', 'nhs.uk', 'gov.uk', etc.); domains such as Hotmail and Googlemail are not acceptable
- Individual accepts responsibility to inform the Informatics HelpDesk when their email address needs to be removed e.g. staff leaving, change of role, long term absence

5.6 Data Protection / Freedom of Information

5.6.1 Email containing personal data are covered by the Data Protection Act 1988 and therefore can be disclosed under Subject Access Request. The Trust will undertake searches of a staff member's email account to process such a request and reserves the right to do so when required.

5.6.2 Al staff must comply with the principles of the Act as follows:-

- To be used for the purpose for which the information was provided
- Be accurate and up to date
- Must not be disclosed to third parties without the express permission of the individual concerned
- Where deemed necessary, be printed and filed in the individual's file and retained as per the NHS Records Management Code of Practice.
-

5.6.3 Emails can be disclosed under the Freedom of Information Request.

5.6.4 All external email will have a disclaimer.

5.7 Unacceptable Use

5.7.1 It is strictly prohibited to send or forward emails containing abusive material including the use of foul language, malicious, libellous, defamatory, offensive, discriminatory in any sense, bullying, intimidating, harassing, racist, obscene or pornographic remarks or depictions about any persons, living or deceased. If you receive an email of this nature, you must promptly notify your Supervisor/Manager.

5.7.2 Where a member of staff receives an email that contains any information as described in section 5.1.1 they must not forward the email but delete it immediately.

5.7.3 Staff should not send unsolicited e-mail messages. The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.

5.7.4 Staff must not send e-mail messages using another person's email account. Where staff need to send an e-mail on behalf of someone else, this must be undertaken using the appropriate tools within Outlook. Staff who are unfamiliar with this functionality in Outlook should contact the Informatics Training Department to book onto an appropriate training course.

5.7.5 Trust email may not be used to purchase anything on behalf of the Trust without specific authorisation, and then only in accordance with the Trust's current procurement policies.

5.7.6 Staff must not leave the Trust email addresses on any websites other than for legitimate and necessary business purposes. Staff must not use their Trust email address to receive mailing lists or newsletters other than for legitimate and necessary business purposes.

5.7.7 Staff must not set up automatic forwarding of Trust emails to addresses external to the Trust. Staff should also consider whether a person who is being sent an email from the Trust has set up auto-forwarding of their email to an insecure email address.

5.7.8 Staff must not use the Trust email system to support or pursue private businesses, for commercial purposes or any form of personal financial gain.

5.7.9 Using the Trust email as detailed in this section may be treated as a disciplinary offence and could give rise to disciplinary procedures.

5.8 Group Account/Shared Calendars

5.8.1 Group email, generic email accounts and shared calendars can be set up. To do this the member of staff must log a request call with the Informatics HelpDesk.

5.8.2 Where a group/generic email or shared calendar is set up, each folder must have a named member of staff who is responsible for the management of the folder.

5.8.3 The named responsible member of staff must ensure that appropriate permissions and access have been granted to the shared folder/email account.

5.8.4 Where a generic e-mail account is set up, the named responsible member of staff must ensure that there are clear procedures for the sending and receiving of emails from that account.

5.9 Retention/Archiving/Deletion of Emails

5.9.1 Staff are responsible for the management of their emails and must routinely delete non-essential email messages as soon as possible on a regular basis.

5.9.2 Any emails that form part of a Trust record must be kept the Trust record e.g. in a department's shared drive and kept for the appropriate length of time as identified in the Department of Health Records Management Code of Practice or the local departmental retention schedule.

5.9.3 When a member of staff has left the Trust, their email account will be made inactive and then deleted.

5.9.4 The archive facility is used to make the inbox and sent box more manageable and is required as the sizes of these boxes are limited.

5.9.5 Where staff have a need to archive their emails, these must not be stored onto an unencrypted hard drive / C drive of any Trust computer. Email archives should be stored on the Trust server in the member of staff's personal folder.

5.10 Personal use

5.10.1 The primary reason for the Trust's e-mail system is to support the Trust's business.

5.10.2 However, the Trust does allow the reasonable use of email for personal use if the following guidelines are adhered to:

- Personal use of email must not interfere with work and be used within approved breaks
- Personal emails must adhere to this policy
- All personal emails must be marked "Personal"
- Personal emails must be stored in a folder named 'Personal'; where there is a need to retain the email after it was received or sent.
- Emails stored in the personal folder must be deleted monthly so as not to clog up the system
- Personal use of email must not be in breach of any Trust policy, or bring the Trust into disrepute

5.10.3 When sending a personal email, staff should ensure that the following disclaimer is included in the email "This email is a personal communication and is not authorised by or sent on behalf of Frimley Health NHS Foundation Trust or any other person or organisation."

5.10.4 Whilst the Trust allows staff to use email for personal use, the Trust reserves the right to monitor staff usage of email, which could entail accessing emails that are personal.

5.10.5 Staff must not use their personal email for Trust business.

5.11 Access to Staff Email Accounts

5.11.1 Where another member of staff needs access to another person's inbox, this must be provided through appropriate access rights and not by sharing a username and password. Where a member of staff is found to have obtained access through the sharing of username and password, the users account may be disabled, and may be viewed as a breach of Trust policy.

5.11.2 The Trust reserves the right to access an individual account when required at all times, in cases without notifying the member of staff.

5.11.3 In some very rare instances (e.g. unplanned sick leave) it may be necessary for the Trust to access or provide access to your Trust email during your absence. Where this is the case, all requests for access to email must be logged by the member of staff's Line Manager with the Informatics HelpDesk.

5.11.4 All requests for access to another person's email will be referred to, considered and approved by the Trust's Information Governance Team.

5.11.5 Trust staff must not share their username and password.

5.12 Copyright/Intellectual Property Rights

5.12.1 Sending an e-mail to more than one recipient constitutes publication and as such is subject to publication laws.

5.12.2 Communications are protected by Intellectual Property Rights which are infringed by copying.

5.12.3 Staff must not breach copyright or licensing laws when composing or forwarding e-mails and its' attachments.

5.12.4 If a message is sent from your account that causes offence or contains inaccurate or libellous information, you will be held responsible, regardless of whether you actually sent the message, unless appropriate permissions have been set up.

5.12.5 When forwarding on an email with copyright content, the sender must ensure they have the permission of the email author.

6. DUTIES / ORGANISATIONAL STRUCTURE

6.1 The Chief Executive has overall responsibility for the Trust's security and confidentiality programme and ensuring that this operates effectively. They delegate operational responsibility to the Director of Finance.

6.2 The **SIRO** will:-

- Ensure that this policy is fully implemented and monitored.
- Ensure that this policy is reviewed periodically.

6.3 The **Information Governance Committee** is responsible for:

- Reviewing and approving this policy and procedure prior to final ratification.
- Review all email associated incidents and escalate

6.4 The **Head of Information Governance** is responsible for:-

- Investigate Information Governance incidents relating to transmission of confidential and/or sensitive data through emails.
- Report the emails related incidents to the Information Governance Committee on a quarterly basis for review as part of the SIRO Report.

6.5 Managers will:-

- Ensure that all of their staff are aware of this policy and understand their responsibilities.
- Monitor that their staff are following this policy.
- Managers must encourage their employees to use their email accounts.
- Where managers are aware that some of their staff are without active email accounts, they must ensure that they cascade important Trust communications to their team, e.g. Rapid Communications, emails alerting staff to new policies and Team Brief.
- In cases where staff members go on a period of sick leave lasting three or more days, managers must compose an appropriate message and forward it to IT HelpDesk requesting that the “Out Of Office” function be activated.
- Identify and provide secure access to equipment that their staff may use to access their emails.

6.6 All Staff must

- Make themselves aware of this policy and are responsible for adhering to it. Anyone found in breach of any aspect of this policy may be subject to disciplinary action.
- Only access the Trust email system if they have been authorised to do so.
- Report immediately to their Line Manager and the Information Governance Team if they have been sent confidential email in error.
- Check their email on a daily basis as they would do with ordinary post and respond in a timely manner.
- To manage the size of a member of staff’s outlook, staff should set up option within Outlook to automatically delete emails in the Deleted Items upon exiting Outlook.
- Staff are responsible for managing their emails within their allocated size limit and this will entail creating folders to store emails that need to be kept and deleting emails that are no longer needed.
- Service their NHSmail account regularly whilst not neglecting to check their Trust inbox on a daily basis.

7. RAISING AWARENESS / IMPLEMENTATION / TRAINING

7.1 The initial awareness of this policy will be raised at Trust staff Induction, staff essential training.

8. MONITORING COMPLIANCE OF POLICY

8.1 Where it is identified a member of staff is not adhering to the guidelines set out in this policy, the Trust reserves the right to take disciplinary action, which may lead to a termination of e-mail account/contract and/or legal action.

8.2 When monitoring staff usage of email, monitoring is undertaken in full consideration of Article 8 of the Human Rights Act 1998 and the Information Commissioners Office “The Employment Practice Code: Part 3 Monitoring at Work.

9. REFERENCES

- Data Protection Act 1998
- Confidentiality Code of Conduct
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Information Commissioner - Employment Practices Data Protection Code: Monitoring at Work(2011).
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000 Telecommunications (Lawful business Practice) (Interception of Communications Regulations 2000

10. APPENDIX

Appendix 1

Sending Email Securely

@nhs.net

@nhs.net

police.uk

gsx.gov.uk

mod.uk

gsi.gov.uk

gse.gov.uk

cjsm.net

Please contact
information.governance@fhft.nhs.uk
for more details

@fhft.nhs.uk

@fhft.nhs.uk

@doctors.net

@yahoo.com

@btinternet.co.uk

@gmail.com

@aol.com

@hotmail.com

Key

This transfer of information is secure.

This transfer of information is not secure. You must encrypt any personal, confidential or sensitive information sent in this way.